Distributed WPA PSK security audit

Александър Станев

OpenFest 5-6 XI 2011
Интерпред, София

Криптографски основи на WPA/WPA2 auth

- Няма разлика в процеса на оторизация при WPA и WPA2
- Масово се използва предварително споделен ключ
- 64 hexadecimal разряда
- 8-63 printable ASCII символа (95)
- PBKDF2(ssid, passphrase)
- 4096 итерации с HMAC-SHA1

Възможни атаки

- Класическият bruteforce е неефективен
- Речникови атаки
- Rainbow атаки (time to memory tradeoff) – при наличие на предварително изчислени таблици за конкретния SSID
- Проблеми с WPA-TKIP – инжектиране на малки пакети (например ARP), декриптиране на целия трафик към клиента. Зависи от QoS(802.11e).

Средства

- Sorbo от екипа на aircrack-ng разработва besside-ng в началото на 2010
- По подобие на wesside-ng, това е средство за автоматизирано прилагане на познатите методи за атака на wireless мрежи, но поддържа и WPA
- Опцията *-s* дава възможност да се изпращат прихванатите 4-way handshakes към отдалечен сървър

wpa.darkircop.org

- Статус на разработката – proof of concept
- Приема captures от besside-ng
- Обработва ги с wpaclean (друго средство от SVN на aircrack-ng)
- Възможност за разпределена атака с aircrack-ng посредством bash скрипта help_crack.sh

Проблеми

- Най-разпространеното средство за прихващане на handshakes е aircrack-ng
- Поддържа само CPU cracking
- Не притежава stateful handshake parsing, което води до наличието на множество false positives при идентифицирането на валиден handshake и false negative при атакуването на handshake-а

Проектът dwpa

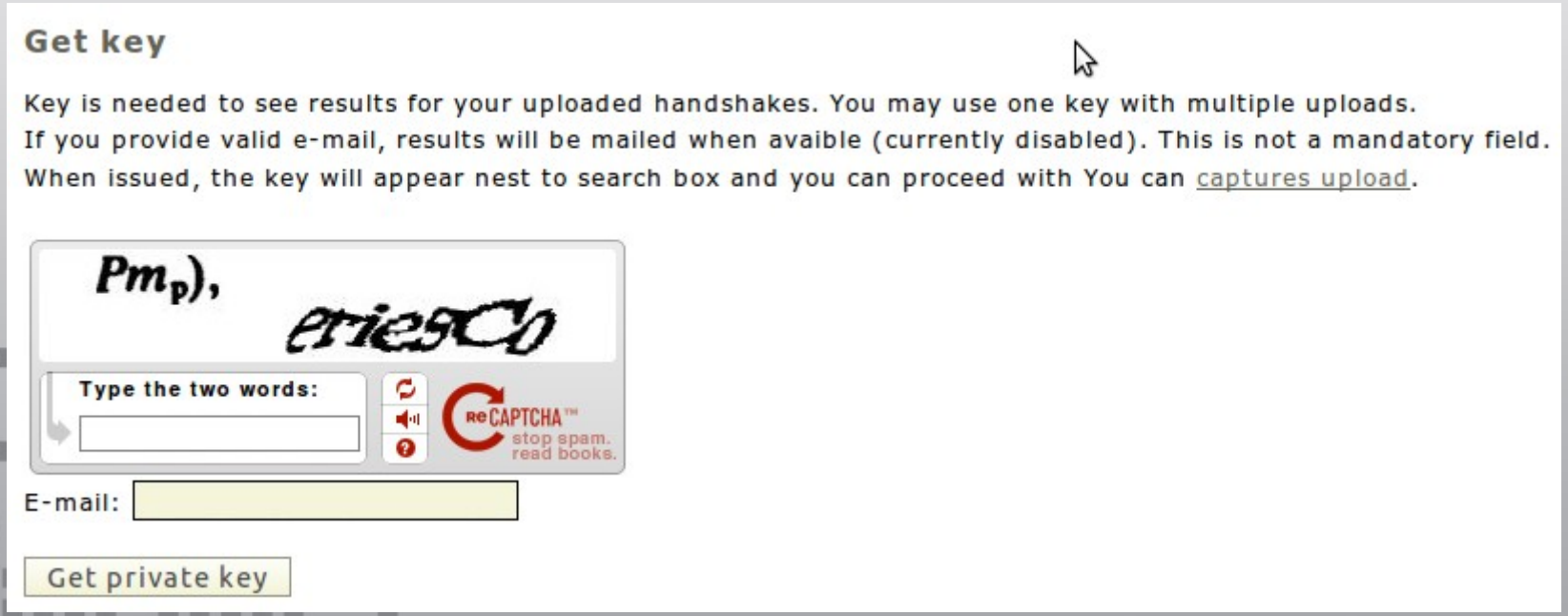
- Пълно пренаписване на сървърната част на besside-ng с направени подобрения и добавени възможности
- Комбинира възможностите на множество проекти в областта
- Отворен код http://sourceforge.net/projects/dwpa
- Жива инсталация http://wpa-sec.stanev.org

dwpa анализатор

- Изпратените packet captures преминават през серия проверки:
- wpaclean за изчистване на ненужните пакети – оставят се eapool и един beacon
- tcpdump разделя отделните мрежи
- pyrit 0.4.1 analyze извършва stateful анализ и гарантира валидността на handshake-а

dwpa ключове

- На потребителите се издават уникални ключове, с които виждат резултатите за единствено изпратените от тях captures



dwpa речници

- Допълнени и подобрени речници с помощта на wlc [http://sec.stanev.org]

wlc_0.2.zip	This is set of tools to help extraction and build of wordlists from hudge set of files. Currently supports raw txt, html and Wikipedia xml.bz2 dump. Extracted words are put in sqlite3 db with additional metadata. Tested with python 2.7, depends on sqlite3 module version 0.2 6 Sep 2011 | README | CHANGELOG | Launchpad

Rule engines!

Dictionary	Word count	Hits
Offensive Security	34239072	0
InsidePro	7789778	0
Wikipedia en	5927677	0
Wikipedia de	5430192	0
Wikipedia ru	2574162	0
Old gold	1560185	544
Wikipedia es	1530155	9216
wp_chit bg	1318369	10040
Wikipedia fr	1295615	10356
OpenWall	1148592	10803
CoW	931005	10903
Slang	510453	10912
C-nets	965	11397

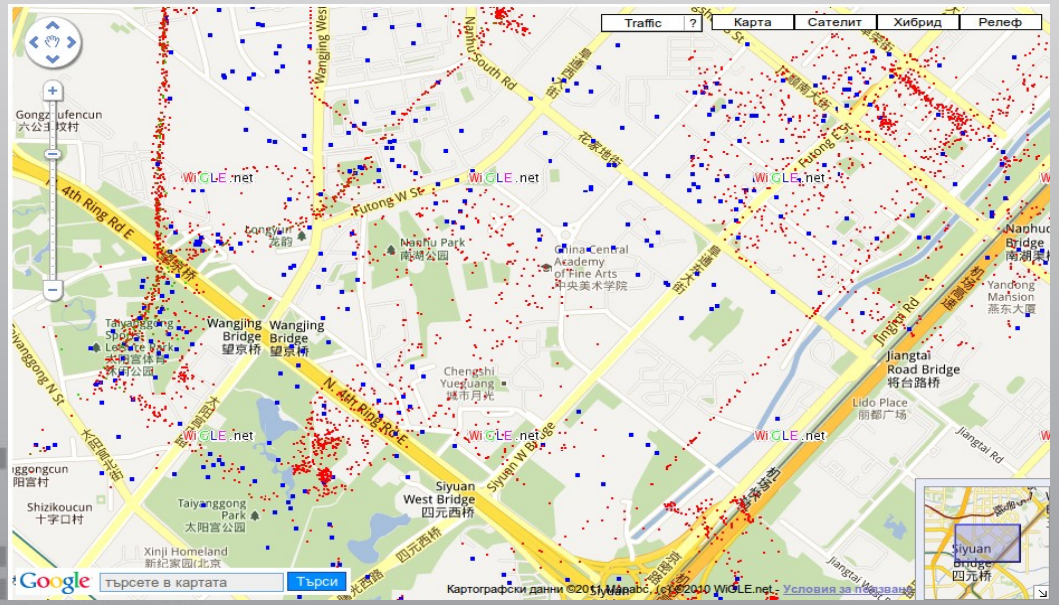
dwpa geolocation

- WiGLE.net съдържа информация за местонахождението на 47`000`000 WIFI AP

BSSID	SSID	WPA key	Get works	Timestamp
48:5b:39:db:b2:a8	ASUS		6	2011-11-03 08:44:31

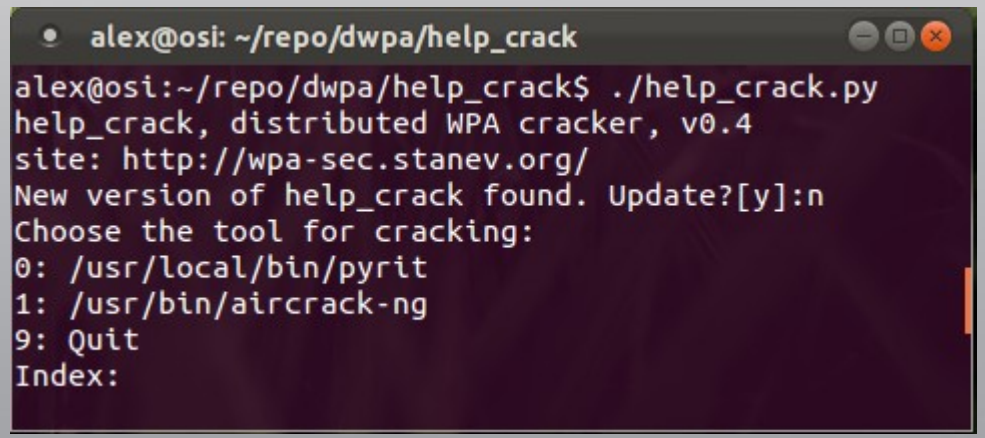
Showing stations 1 through 1 of this query.

map it	netid	ssid	comment	name	type	freenet	paynet	firsttime	lasttime	flags	wep	trilat	trilong	dhcp	lastupdt	channel	bcninterval	qos	userfound
Get Map	48:5B:39:DB:B2:A8					?	?	2011-02-19 08:00:28	2011-08-28 08:56:43		?	39.98281479	116.46535492	?	20110828090213			0	N

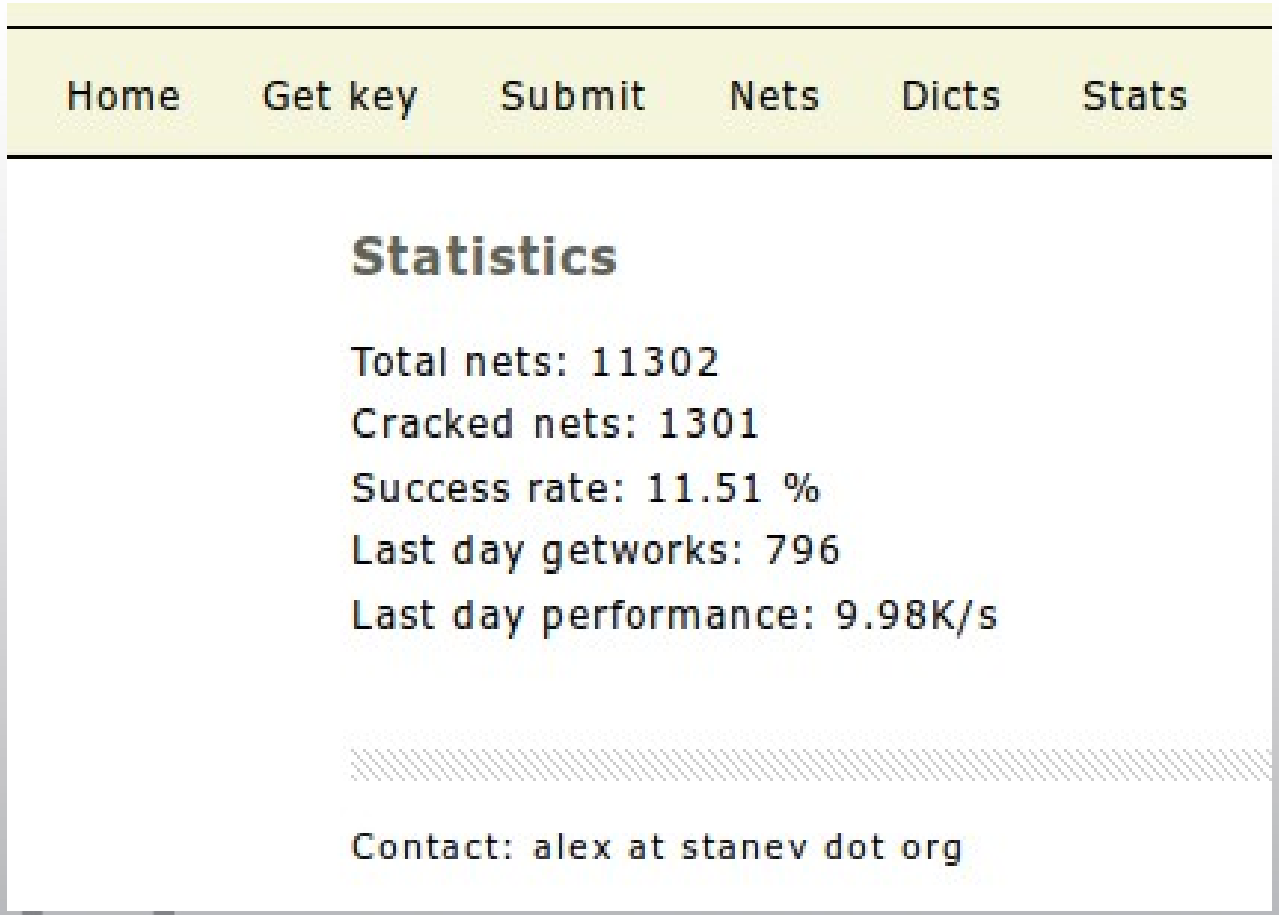


dwpa help_crack.py

- Python скрипт, който организира изтеглянето на packet captures и речници
- Използва aircrack-ng, pyrit или oclHashcat-plus за изпълнение на атаката
- При успех изпраща обратно информация към сървъра за открития PSK
- Многоплатформен
- Онлайн обновяване



dwpa статистика



dwpa развитие

- Възможност за изключване на мрежи от базата
- Работа с повече от един capture за дадена мрежа
- Използване на събраната база за подобряване на opensource средствата
- Добавяне на нови crackers
- Android приложение
- Повече: http://svn.code.sf.net/p/dwpa/code/doc/TODO

Подобряване на сигурността на WIFI AP

- Използвайте WPA2-AES
- Нестандартен SSID за потискане на rainbow атаки
- Дълги, нестандартни PSK, планирана промяна през определен интервал от време
- EAP extensions при WPA/WPA2-Enterprise – оторизация със сертификати чрез authorization server

Въпроси? Идеи!

http://wpa-sec.stanev.org

http://sourceforge.net/projects/dwpa

alex@stanev.org